

**BY ORDER OF THE COMMANDER
94TH AIRLIFT WING**

94TH AIRLIFT WING INSTRUCTION 33-202

24 DECEMBER 2009



Communications and Information

COMSEC OPERATIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 94 CF/SCBP

Certified by: 94 CF/CC
(Maj. Kayla Sailer)

Pages: 9

This Instruction implements AFKAG 1, Air Force *Communications Security* (COMSEC) *Operations* and AFI 33-201 Volume 1 and 2, *Communications Security (COMSEC), User Requirements*. It establishes additional guidelines and procedures for COMSEC operations for the 94th Airlift Wing, specifically the use and protection of Electronic COMSEC keying materials as it is utilized with the Data Management Device – Power Station (DMD-PS), Simple Key Loader (SKL) and other crypto fill devices. This instruction applies to all personnel assigned to the 94th Airlift Wing and tenant organizations assigned at Dobbins ARB, GA that have access to and/or receive COMSEC material, equipment and aids from the 94th Airlift Wing COMSEC Accounting Office (CA/669515). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) by filling out the Air Force Form 847, **Recommendation for Change of Publication**; route AF Form 847 directly to 94 CF/SCBP at Dobbins Air Reserve Base, Georgia.

Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims.afrims/>.

1. Management of COMSEC Materials. This section provides guidance on the use of the Data Management Device and Simple Key Loader and their role in managing COMSEC material within user accounts. It also provides guidance on the use of Electronic keying material.

1.1. Data Management Device – Power Station (DMD-PS). The DMD-PS is software written for the AF that provides the COMSEC element (user account) a computerized way to manage their COMSEC materials.

1.1.1. Required Use. All COMSEC elements holding two or more COMSEC keys or who hold physical materials and electronic keys will use a DMD-PS to manage their account. The DMD-PS is just software and it can be loaded onto any stand-alone system.

1.1.2. Accountability. All laptops use to run the DMD-PS software must be managed through the Air Force Equipment Management System (AFEMS)'s Asset Inventory Management (AIM) module or the COMSEC Material Control System (CMCS). If you were issued a DMD-PS laptop from the COMSEC Office it will be managed through CMCS. All other DMD-PS laptops will be managed through AIMs. Regardless of the management system, all DMD-PS laptops are accountable as ALC 4 COMSEC.

1.1.3. Restrictions.

1.1.3.1. DO NOT load DMD-PS on a SIPRNET system.

1.1.3.2. Do not transfer or store Red Key on the DMD-PS. This constitutes a violation of National COMSEC Policy and must be reported as a COMSEC incident.

1.1.4. Capabilities. The DMD-PS provides the following capabilities:

1.1.4.1. The DMD-PS provides the capability to create Packages (mission), Platforms (aircraft) and Equipment which is required for the keying of some ECUs (ARC-164). In addition the DMD-PS can manage expiration dates and destruction of electronic key.

1.1.4.2. The DMD-PS can also manage every aspect of physical COMSEC material receipt, accounting and destruction.

1.1.5. Classification. The DMD-PS is classified at a minimum SECRET because IAW COMPUSEC rules the system takes on the same classification as the media used in it. The Black Key Floppies are classified SECRET so the DMD-PS is classified SECRET. The effective date information for the material listed in the DMD-PS is classified CONFIDENTIAL.

1.1.6. Inventory. The DMD-PS will be placed on the COMSEC Physical Inventory (CPI), AFCOMSEC Form 16, *Daily Inventory*. Use the following format:

1.1.6.1. Record the Short Title on the inventory as "DMDLaptop 1"

1.1.6.2. In the Serial Number block, record the letter "C" plus the last four of the laptop serial number; example "C2345."

1.1.7. Storage. The DMD-PS will be stored in a GSA approved container.

1.1.8. Disposition of DMD. Contact the COMSEC Office at ext 5-5154 to arrange for the disposition of the DMD-PS laptop. A destruction report will be required for all applicable COMSEC material and the COMSEC Manager must witness the removal the electronic keys, the database and Power Station software.

1.2. Electronic Key. The National Security Agency and the Air Force have directed that all possible paper COMSEC key-tape be converted to electronic key and that electronic key be

used whenever possible. Grissom ARB has been the lead in electronic key use; however, formal written policy from the AF has lagged behind technology. This instruction is designed to provide guidance for the use of electronic key and additional requirements that are not covered in existing instructions.

1.3. Issuing Electronic Key to COMSEC Users. All COMSEC users that require keying material for use in a End Cryptographic Unit (ECU) will receive their material as electronic key (if available) by one of these two forms:

1.3.1. Black Key Floppy. This is a floppy disk that is created by the Electronic Key Management System (EKMS) located in the wing COMSEC office. This disk contains Red (classified) COMSEC key that has been encrypted with a unique Transfer Key (TrKEK) which turns the Red key into Black (unclassified) data. The Black Key Floppy is considered classified SECRET, Accounting Legend Code (ALC) 4 because it was created by a SECRET high computer. However, the data on the floppy is considered unclassified. This floppy is used to import the Black Key into the Data Management Device – Power Station (DMD-PS).

1.3.2. SIPRNET E-mail. Accounts with access to the SIPRNET can receive their key via e-mail. The zipped file will contain two files; one text file that is the data that is filled in to the DMD-PS, so that text file is important; and one XML file which is the encrypted key data. These files can be downloaded onto a classified floppy disk, a classified thumb (USB) drive or a classified CD-R/RW. Then follow the XML file import procedure for the DMD-PS and import the data into the DMD-PS.

1.4. Simple Key Loader (SKL). The AF has stated that the SKL is the fill device of choice. The SKL will be loaded with the same TrKEK that the Black Key issued to it is encrypted with and when Black Key is issued to a SKL from a DMD-PS the Black Key is sent to the side of the SKL that is also encrypted with the Crypto Ignition Key (CIK). For this reason the AF considers this key to be “super encrypted” and thus less vulnerable. The following procedures will be followed to account for and use the SKL.

1.4.1. SKL Usage. The SKL is the only fill device that is to be used with 94 AW ECU's. Due to serious security concerns the KYK-13 is NOT to be used except for emergencies. Although other units, especially active duty units, are using the KYK-13 because they are easier, lighter, etc. that is no reason to regress back to exposing RED (classified) key when a SKL works just as well and is more secure.

1.4.1.1. The SKL allows for 10 users and one System Security Officer (SSO).

1.4.1.2. SKL passwords should be at least 9 characters with upper and lower case and at least one number.

1.4.1.3. Change SKL passwords at least every 90 days.

1.4.1.4. For small COMSEC elements (10 or less users) use one password per user.

1.4.1.5. For larger elements and for aircrew; group passwords are authorized.

1.4.1.6. SKL passwords are UNCLASSIFIED but should be written down and stored on a SF-700 (Security Container Information) in a secure location.

1.4.2. SKL Audit Data Process. DMD-PS version 2.1 and SKL version 4.0 provides the ability to upload the SKL audit data to the DMD-PS and to archive the audit data so it can be sent to the main COMSEC account. The following are guidelines for uploading the audit trails. Remember failure to review or upload the audit data is a reportable COMSEC deviation.

1.4.2.1. The SKL Audit can only be sent through the fill port at a max rate of 2400 baud. The Audit Full indication appears at about 200K or 10% of the maximum audit capability of the SKL. Failure to upload the audit soon after the Audit Full appears increases the time it will take to upload the audit data.

1.4.2.2. The audit data can be uploaded at any time but should be uploaded to the DMD-PS as soon as possible after the Audit Full indication appears on the SKL.

1.4.2.3. For daily users, upload the audit data at least monthly.

1.4.2.4. For periodic users, upload the audit data at least quarterly.

1.4.2.5. Archive the audit data according to the SKL serial number. DMD-PS will request the serial number of the SKL. It is important that you provide the correct information.

1.4.2.6. Archived audit data will be sent to the main COMSEC account. They can be sent via SIPRNET or copied to a floppy disk or CD-RW. The audits can be delivered to the main COMSEC account anytime but at least when the destruction certificates are brought to the account at the beginning of each month.

1.4.2.7. SKL audit data is UNCLASSIFIED/FOR OFFICIAL USE ONLY but any media that the archived data is copied to will retain the classification of the DMD-PS which is SECRET.

1.5. KYK-13. This instruction places a restriction on the use of the KYK-13 to emergencies only; in addition when a KYK-13 is used for emergency purposes the following procedure will be followed:

1.5.1. Notify the COMSEC managers of the nature of the emergency that warrants the use of a KYK-13.

1.5.2. An Electronic Key DRC (AF Form 3137, *General Purpose*) must be used. Since you will be converting BLACK key to RED key you need to document that issue and destruction just as if you were pulling a segment out of a canister.

2. Record Maintenance and Disposition. This section provides guidance on the use of the DRC for electronic keying material managed by the DMD and SKL.

2.1. Disposition Record Card (DRC) use. The DRC is a legacy document that records the issuing and destruction of paper-tape keying material. However the current AFSSI 3021, *OPERATIONAL SECURITY INSTRUCTION FOR THE AN/CYZ-10/10A DATA TRANSFER DEVICE (DTD)* and the AFSSI 3041, *OPERATIONAL SECURITY INSTRUCTION FOR THE AN/PYQ-10 SIMPLE KEY LOADER (SKL)* implies that the DRC is still required when using electronic key but does not direct how it is to be used. Until further direction is received from AFCA or HQ AFRC the following procedure will be followed for the use of the DRC.

2.1.1. When you receive electronic key from the COMSEC Office you will also receive a DRC for each short title. Process the electronic key immediately into the DMD-PS. Once the key(s) has been brought into the DMD, “Z” out all issue dates on the DRC and write on the diagonal line of the Z “Issued to the DMD #, date, Init.” The SKL audit trail will serve as an official record, when it is used to load key into the ECUs. The destruction blocks on the DRC will be completed when segments are destroyed from the DMD-PS database.

2.1.2. The DMD-PS stores the electronic key as if it was a key “canister”. Also, the DMD-PS does not have audit capability. Therefore, use the DRC whenever key is “**issued**” to a COMSEC user via a SKL and the SKL becomes the storage container for that particular key.

2.1.2.1. Document the issue of individual key segments to the SKL just as if it was a paper key segment issued to a KYK-13.

2.1.2.2. If a whole key is issued to a SKL “Z” out the whole DRC and write on the DRC “All keys issued to SKL S/N #####”.

2.1.2.3. If the same key is issued to more than one SKL identify each SKL serial number.

2.1.2.4. Document destruction of key segment(s) only when they are deleted off of the DMD-PS database.

2.2. Red Key. If Red key is pulled through a KOI-18 into the SKL a DRC is required for that key. However, if that Red key is issued to a DTD or KYK-13 for any reason, an Electronic Key DRC is required for each device that holds the Red key.

3. Physical Security Requirements. This section establishes guidance for the use and storage of the SKL and its associated CIK, as well as other peripheral devices utilized with the SKL.

3.1. SKL and CIK .

3.1.1. The SKL retains the highest classification of the key stored in it when these two conditions are met (TPI rules apply):

3.1.1.1. The CIK is inserted

3.1.1.2. Any user is logged into the SKL.

3.1.2. The SKL and CIK are considered UNCLASSIFIED when separated. Separation implies stored in separate locked containers.

3.1.3. The SKL is an ALC 1 item and must be accounted for on a COMSEC Daily Shift Inventory.

3.1.4. The SKL CIK is not a COMSEC item but for accounting purposes it is recommended that it be inventoried if not stored with the SKL in a GSA approved container.

3.2. USB Keyboard and mouse use with the SKL. The SKL is designed to accept a USB keyboard and mouse if desired. However do not use a USB keyboard to input classified data of any kind. The USB ports have not been EMSEC certified and are not authorized for use with classified information.

4. Reporting COMSEC Deviations. This section establishes guidance when reporting COMSEC Deviations.

4.1. Reporting Procedures. Report COMSEC deviations IAW AFSSI 4212, *Reporting COMSEC Deviations*; in addition CROs will follow these procedures:

4.1.1. Contact your unit commander as soon as possible and notify him/her that a possible COMSEC deviation has taken place. DO NOT discuss details on a non-secure phone line.

4.1.2. Contact the base COMSEC office at ext 5-5154 and request to go secure voice. A Secure Voice device must be used for a call of this nature. If the reporting CRO or user is not able to pass the information in a secure mode, he/she should report the incident in person to the COMSEC Manager immediately.

4.2. Reportable Information. Report the following information:

4.2.1. Organization and person notifying the account of a possible incident.

4.2.2. Time and date of the COMSEC deviation.

4.2.3. A brief description of the incident.

4.3. Written Statements. All individuals involved should prepare a written statement describing the COMSEC deviation as they know it. Remember details of a COMSEC incident could be classified, so written statements should be written on a classified computer and marked appropriately.

4.4. Notification. The COMSEC Manager will determine (using AFSSI 4212) if the incident is reportable and notifies the 94 CF/CC and 94 Wing Commander of the incident either in person or via secure phone.

4.5. Practice Dangerous to Security (PDS). If the incident is a PDS and is not reportable, the COMSEC Manager or Alternate will notify the HQ AFRC Command COMSEC manager (AFRC/CA629600) via SIPRNET e-mail of the details of the PDS.

5. Controlled Cryptographic Items. This section establishes additional guidance and provides procedures in the management of CCI equipment as it relates to COMSEC management and operations.

5.1. General Information. CCIs are used to protect voice, record, and data communications processed by traditional national security telecommunications systems, and also to provide network security for automated information systems.

5.1.1. The secure telecommunications and information handling equipment and associated cryptographic components designated "Controlled Cryptographic Items (CCI)," employ a classified cryptographic logic in their design. However, the hardware or firmware embodiment of that logic is unclassified but controlled. The associated cryptographic engineering drawings, logic descriptions, theory of operation, computer programs, and related source data remain classified.

5.1.2. The control requirements set forth in this operating instruction are necessary to guard against preventable losses of unkeyed CCIs to an actual or potential adversary. See AFI 33-201, Volume 5 paragraph 14, for detailed procedures for reporting incidents involving unkeyed CCIs.

5.2. CCI Database. The COMSEC Accounting Office maintains a database of all CCI serviced by the Dobbins ARB COMSEC Account, CA669515. This database is updated as required by the CRO/SVRO of each organization. Whenever CCI is received and/or transferred the COMSEC Office will be provided the location of the equipment.

5.3. Receiving Unkeyed CCI.

5.3.1. COMSEC Material Control System. The COMSEC Accounting Office is the central focal point for the receipt and disposition of all CCI accountable within the CMCS. When an organizations serviced by the COMSEC Office expects a package, the COMSEC Manager will be notify in writing or via email of the pending delivery. The receiving organization will also give the shipping authority the physical address and account number of the COMSEC Accounting Office. The package will be shipped to the COMSEC Accounting Office address and marked for delivery to the receiving organization.

5.3.1.1. When the package arrives, the COMSEC Manager will inspect the package for tampering, complete all required documents, process the CCI in LCMS/CUAS and schedule pickup with the receiving organization.

5.3.1.2. Upon receipt, the receiving organization will place the CCI on the Daily/Shift inventory, AFCOMSEC Form 16, *COMSEC Account Daily Shift Inventory* and then place in a GSA approved container for storage.

5.3.2. Air Force Equipment Management System. Base Supply will handle the receipt of CCI accountable within the AFEMS. Once CCIs arrive on Dobbins, Supply personnel will contact the COMSEC Accounting Office at ext 5-5154. The CCIs will be delivered to the COMSEC Accounting Office. The COMSEC Manager will inspect the package and complete all required documentation. Once completed, he/she will release it to the appropriate organization.

5.4. Shipping Unkeyed CCI.

5.4.1. COMSEC Material Control System. All CCI accountable within the CMCS will be shipped by the COMSEC Accounting Office. Organizations needing to ship CCI will notify the COMSEC Office for instructions.

5.4.2. Air Force Equipment Management System. Base Supply will handle the shipping of all CCI accountable within the AFEMS. Prior to arranging for the shipment of AFEMS CCI, notify the COMSEC Accounting Office, and provide a list of all CCI being shipped.

5.5. Inventory.

5.5.1. The COMSEC Manager will perform an inventory of all CCI accountable within the CMCS in May and November of each year.

5.5.2. The CRO and/or Unit Equipment Custodians will perform an inventory of all CCI accountable within the AFEMS every 12 months. The periodic interval between successive inventories may never exceed 12 months.

5.6. Storage. There are many factors that govern the proper storage of CCI. Follow the guidance listed in AFI 33-210, Volume 5 for detailed instructions on unkeyed CCI and

AFKAG 1, Air Force Communications Security (COMSEC) Operations for keyed CCI. The paragraphs below provide limited guidance for Dobbins ARB personnel.

5.6.1. Store CCI accountable within the CMCS in a GSA approved container whether keyed or unkeyed. Contact the COMSEC Manager to arrange for storage if you have CCI and no GSA approved container.

5.6.2. Store all other unkeyed CCI where it will be afforded protection at least equal to that normally provided to other high value or sensitive material. The protective measures employed must reasonably guard against attempts by individuals to gain access to the unkeyed CCIs with the intent of committing acts of theft, sabotage, or tampering.

5.7. Keying Restrictions. Prior to receiving COMSEC keying material for CCIs, the CRO will provide the COMSEC Accounting Office with proof of accountability via the Custodian Authorization Custody Receipt Listing (CA/CRL).

6. Cryptographic Access Program (CAP). All personnel that have a need for access to cryptographic information, material and equipment, must be enrolled in the CAP.

6.1. Roles and responsibilities.

6.1.1. The COMSEC Manager and Alternate. Are the CAP Administrators for the 94 AW and all units that receive COMSEC from CA669515. The CAP briefing will be included in the CRO/SVRO training. Upon completion of the training, all users must sign the AFCOMSEC Form 9, *Cryptographic Access Certificate (PA)* to receive access to crypto. The COMSEC Manager will process the AFCOMSEC Form 9, through AFCA and input them into the COMSEC Management System (CMS). A copy of the AFCOMSEC Form 9 will be maintained in the COMSEC Accounting Office.

6.1.2. The COMSEC Responsible Officer/Secure Voice Responsible Officer will inform the COMSEC Manager when unit member need to be added or removed from the CAP. This notification of changes by the CRO/SVRO, must be provided in writing; email notification is acceptable.

7. Adopted Forms.

AFCOMSEC Form 9, *Cryptographic Access Certificate (PA)*,

AFCOMSEC Form 16, *COMSEC Account Daily Shift Inventory*

AF Form 3137, *General Purpose*.

HEATH J. NUCKOLLS, Colonel, USAFR
Commander

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFKAG-1, *Air Force COMSEC Operations*,

AFKAG-2, *Air Force COMSEC Accounting Manual*,

AFI 33-201V1, *Communication Security (COMSEC)*

AFI 33-201V2, *Communication Security (COMSEC) User's Requirements*

Air Force System Security Instruction (AFSSI) 4212, *Reporting COMSEC Deviations*

COMSEC Policy Message 08-01, Red Key On DMD-PS, DTG 041634Z FEB 08

Abbreviations and Acronyms

AFEMS—Air Force Equipment Management System

CAP—Cryptographic Access Program

CCI—Controlled Cryptographic Items

CMCS—COMSEC Material Control System

COMSEC—Communication Security

CPI—COMSEC Physical Inventory

CRO—COMSEC Responsible Officer

DMD—PS- Data Management Device – Power Station

ECU—End Cryptographic Unit

SKL—Simple Key Loader

SVRO—Secure Voice Responsible Officer